6. A Technical Overview of the Lucent Managed **Firewall**
Lucent Managed **Firewall** A Technical Overview of the Lucent Managed **Firewall** This documen
technical overview of the Lucent Managed **Firewall** architecture. Key technical features and ...
www.sims.berkeley.edu/academics/courses/is250/s99/vendors/lucent/lmf_techni - April 14, 199

Lucent Managed Firewall
Version 2.0

A Technical Overview of the Lucent Managed Firewall

This document provides a technical overview of the Lucent Managed Firewall architecture. Key technical features and potential application scenarios are also discussed.

This document assumes that the reader possesses a basic understanding of IP networking technology and firewall concepts. For an introduction to firewall concepts, please read "Firewalls and Internet Security, Repelling the Wily Hacker," by William R. Cheswick and Steven M. Bellovin and "Intranet and Internet Firewall Strategies," by Edward Amoroso and Ronald Sharp.

Firewalls — The Lucent Architecture

Capitalizing on Bell Labs' experience and expertise in the design, development, and implementation of network security technologies, Lucent Technologies introduces version 2.0 of the Lucent Managed Firewall, the first element of an Internet security platform from Lucent that provides a robust foundation for secure Internet, intranet, extranet, virtual private networking, and e-commerce applications.

The Lucent Managed Firewall architecture consists of two elements:

- ***The Firewall appliance*** a small "black box" built using Bell Labs patent-pending technology that can be positioned between network elements to provide the fundamental security functions
- ***The Security Management Server*** software, which resides on a remote server and handles configuration of multiple firewalls, management of security policies, and collection and analysis of audit data

This architecture was designed to be intrinsically secure. The firewall function is physically separated from its management server, with the firewall code running on Inferno™, a small, highly efficient and highly secure Bell Labs-developed operating system. The separate Security Management Server software, on the other hand, runs on Windows NT™ and Sun Solaris™ platforms, giving customers freedom to choose the machine and platform that best suits their budget and current operating environment.

These elements are described in greater detail below.

The Lucent Managed Firewall Appliance

Hardware

The firewall appliance hardware consists of a small "black box" processor (also affectionately referred to as the "brick") based on the Intel Pentium platform.

The initial release of the brick is equipped with three autosensing 10/100Base-T Ethernet interface cards and can be positioned between any type of Ethernet-based network elements (e.g., routers, hubs, switches, servers, PCs). Because the brick is a bridge-level device, these network interfaces do not have IP addresses, thus rendering the brick invisible to the other network elements[1].

The brick has no monitor, keyboard or hard disk. Other than a floppy disk drive for initial software boot, it has a minimum of moving parts (an on/off switch and a power supply fan). The brick initially boots from a floppy diskette that is created by the Security Management Server. Boot images subsequent to initial boot can be loaded from FLASH RAM in about 30 seconds.

Software

The firewall software that runs on the brick is based on the Inferno™ operating system, a small, highly efficient and highly secure Bell Labs-developed operating system. The firewall code — which is simple and small — is imbedded within the Inferno™ operating system kernel. The operating system itself has no user accounts or file system to be hacked. The entire firewall software resident on the brick fits on a single 3.5 inch floppy diskette.

The brick communicates with its Security Management Server using IP. Accordingly, the brick must be assigned a logical IP address. To further preserve network invisibility, the brick can be configured to communicate only with the Security Management Server's network address, silently dropping all other communication attempts and thus remaining invisible to all other network addresses. All communications between each brick and the Security Management Server are encrypted and authenticated using native Inferno™ encryption and authentication mechanisms (Diffie Hellman for key exchange, ElGamal for digital signatures and signature verification, and Triple DES for session encryption).

[1] The appliance must be visible to the Security Management Server's IP address on at least one physical interface, but can be invisible at the network layer to network elements on the other two physical interface ports.

For more information on the Inferno operating system, please refer to the Inferno web site (http://www.lucent.com/inferno).

The firewall software in the brick consists of the following modules, proxies, and applications:

Decision Module

The brick works with data at the lowest level — the IP packet. The decision module extracts information from the IP packet and applies a set of rules — derived from the security policy — to this information to determine whether or not to allow this packet to pass through the firewall. Information within an IP packet that is used to make access control decisions includes source and destination IP address, source and destination TCP or UDP port number, and packet type (i.e., protocol number). In addition, time-of-day, day-of-week, direction of access, physical Ethernet port, and existing session information can be used to determine whether or not a packet is allowed to pass.

If the decision is to permit the packet to pass, the decision module determines which Ethernet port(s) to send the packet to. If the decision is that the packet requires additional services, such as application proxy services or strong authentication services, it is passed to a local or remote proxy application[2].

Session Cache Module

The patent-pending session cache module retains the access control decision result for use with future packets from the same session. When a packet that is part of an established session arrives at the firewall, the decision module can first check the session cache to determine if the packet is authorized, rather than having to apply the entire list of rules (security policies) against each packet. This provides superior throughput and security because it allows the firewall to quickly and securely identify authorized packets associated with a given session.

Audit Module

The audit module records the start and end of a session. It extracts information from the session cache to uniquely identify each session, and it records:

- Start and stop times
- Action taken
- Statistics, such as number of bytes and packets passed

The audit module bundles this information into an audit message and sends it to an awaiting audit server, located on the Security Management Server.

[2] Application proxies available in a subsequent release.

Application Proxies

In a subsequent release, the Lucent Managed Firewall will provide application proxies for strong authentication for select services, such as http, telnet, and ftp. The application proxies are integrated with a Lucent authentication agent capable of communication with Security Dynamic's ACE/Server™ (for support of SecurID™) and with a RADIUS server, such as Lucent's RADIUS Authentication Billing Manager.

Administration Applications

The administration applications permit the security policies to be remotely loaded in the brick from the Security Management Server over an authenticated and encrypted session. Each security policy's digital signature is verified before the policy is loaded (the policies are digitally signed by the Security Management Server using the firewall administrator's certificate when created or edited). The administration applications also provide system status information.

The Security Management Server

The Security Management Server software provides the tools to manage the security policies of multiple security zones across multiple firewalls.

The software runs at the application layer using hosted Inferno™ on Windows NT™ and Sun Solaris™. As a result, customers are free to choose the machine and platform that best suits their budget and current operating environment.

The Security Management Server implements and enforces a rigorous administrator privilege model. Two categories of administrators can be created: system administrators and security zone administrators. System administrators control the entire system infrastructure (such as which security zones are applied to which bricks), while security zone administrators control only their specific security zone. The privilege to create additional administrator accounts can be assigned to specific administrators. Within a security zone account, the security zone administrator can be assigned create, create/edit, or create/edit/load privileges for managing the security policy within that security zone. The privilege model is maintained entirely within the Security Management Server and is not reliant upon OS-level user accounts or authentication.

The primary components of the Security Management Server software are hosted Inferno daemons, Java™ server-side applications, and a graphical user interface.

Hosted Inferno Daemons

The hosted Inferno daemons act as the interfaces between the firewall appliance and the Java™ server-side applications and provide essential services, such as encryption and end-

user authentication. The daemons include an:

- Administrative daemon
- End-user authentication daemon
- Logger daemon
- Filter daemons

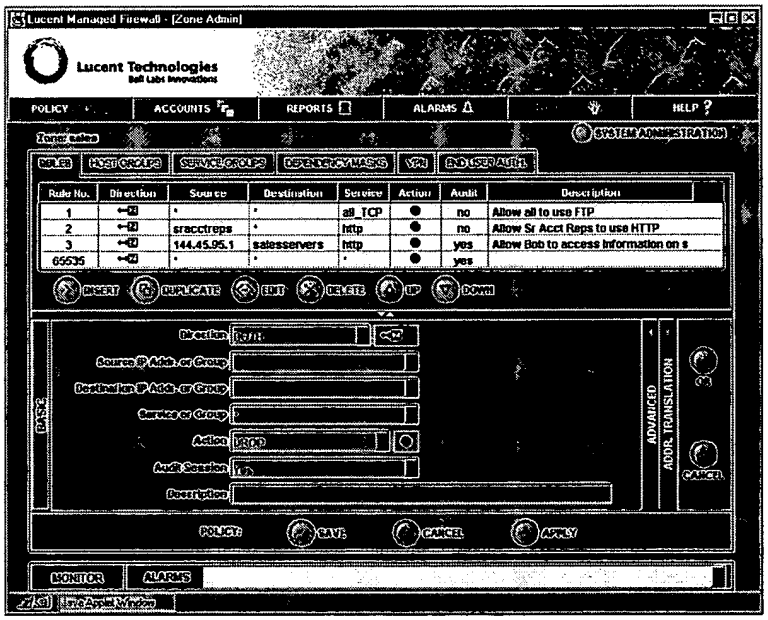
Java™ Server-side Applications

The Java™-based applications include:

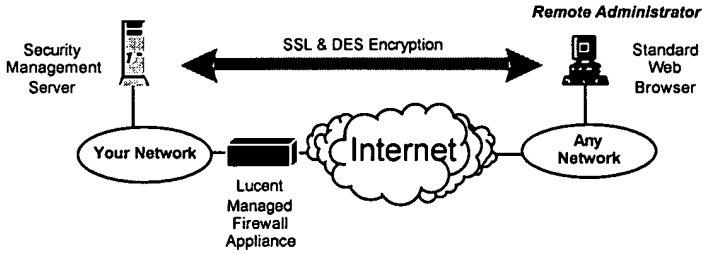
- Administrative application
- Query and reporting application(s)
- Alarm application

Graphical User Interface

The GUI is implemented by Java™ applets executing in a browser on the user's desktop.



An administrator can remotely access the Security Management Server from a PC anywhere on the network, as illustrated below, if the organization's security policy will permit.



The administrator's login is protected by Secure Sockets Layer (SSL) encryption. The server has an X.509 digital certificate to allow the administrator to verify the server's identity. Lucent provides a free server Digital ID from VeriSign. Following administrator login, the Java™ applets are downloaded to the administrator's desktop environment and a key exchange is performed via the encrypted SSL link. Subsequent communications between the Java™ applet and the Security Management Server are also encrypted using DES.

Security Zones

Using patent-pending technology, the Lucent Managed Firewall supports multiple security policy zones. Control of each security policy zone can be restricted to one or more security zone administrators. Using this feature, a network can be easily segmented into several distinct security zones, where control over each segment's security policy can be delegated to a different security zone administrator. The Lucent Managed Firewall ensures that each security zone administrator can access and control only their respective security zone, as the various administrative roles that are permitted follow the concept of least privilege. In situations involving multiple firewalls, it is easy to apply the same security policy to multiple firewalls from one Security Management Server. This was done by defining security policies logically, not physically or geographically.

Within a security zone, the Security Management Server maintains separate security policies, audit logs, and reports for the zone. If the security zone is applied to many firewall appliances, the Security Management Server provides an *integrated* view of all activity for the logical security zone, rather than separate logs and reports for each physical firewall.

A security zone can be applied to either one or more physical interfaces on the brick or to a collection of network addresses on a physical interface.

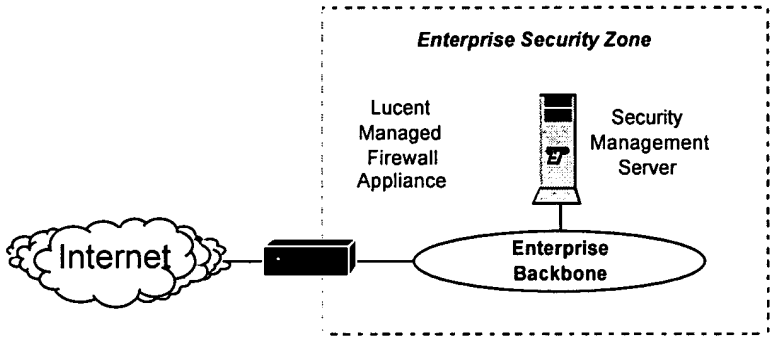
These features allow Internet Service Providers (ISPs) to manage multiple customer firewalls with a single Security Management Server. Furthermore, each of an ISP's customers can have separate security policies, audit logs, and reports. The Security Management Server integrates with the ISP's existing management infrastructure.

Application Scenarios

The Lucent Managed Firewall is flexible, so it can be configured to meet the unique needs of individual customers. A variety of configuration options are shown below.

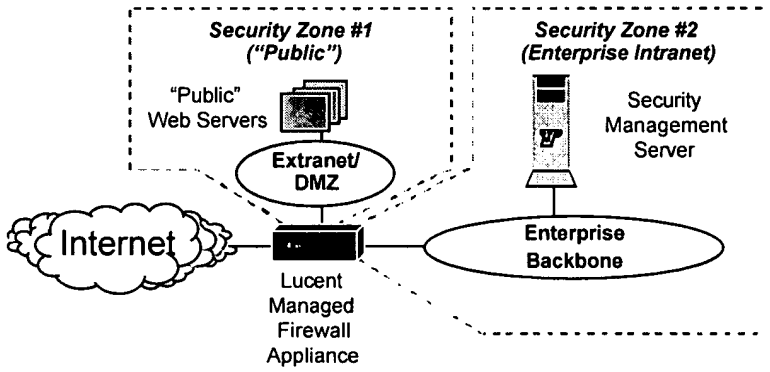
Gateway Perimeter Configuration

For example, the Lucent Managed Firewall can be configured to operate in a classical gateway perimeter setting to protect an enterprise network from the Internet.



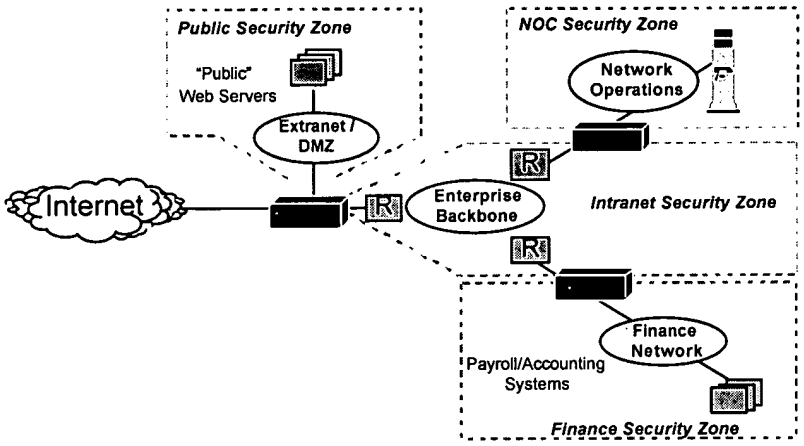
DMZ Configuration

Using the three physical ports on the firewall appliance, the Lucent Managed Firewall can be used to create a "demilitarized" zone (DMZ) or "public" zone to separate an enterprise's public web servers from sensitive enterprise intranet servers. In this configuration, the firewall's unique security zone feature can be used to allow one administrator to control the security policy for the public security zone without giving that administrator any access to or knowledge of the enterprise intranet security zone.



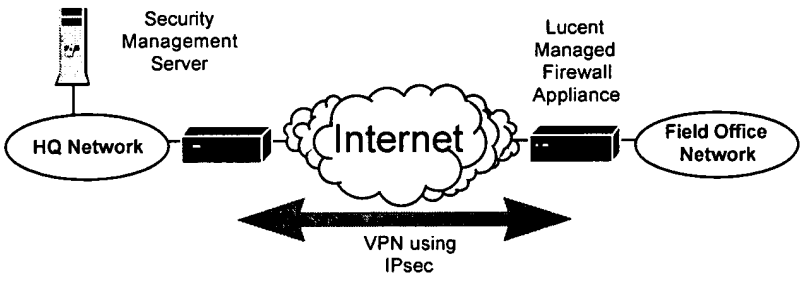
Intranet Configuration

Enterprises searching for cost effective intranet security can use multiple firewall appliances to meet their needs. In this type of configuration, one Security Management Server can be used to control several security zones within the enterprise intranet.



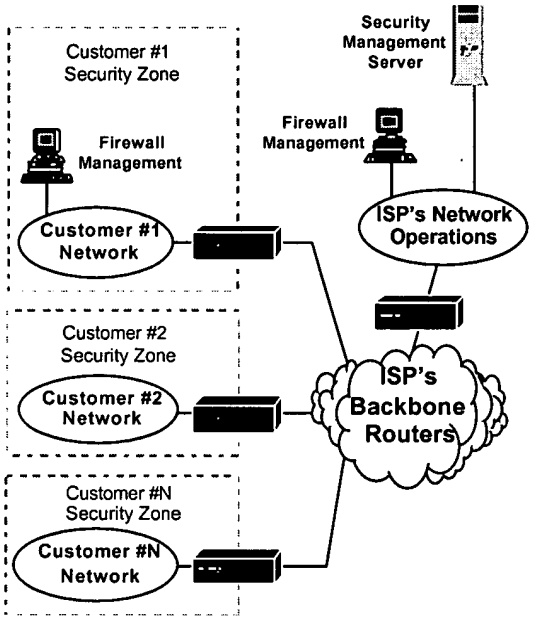
VPN Configuration

The Virtual Private Networking (VPN) feature of the Lucent Managed Firewall can be used by enterprises (or their Internet Service Providers) to replace costly dedicated or private circuits connecting remote offices with less expensive Internet service. The VPN feature implements IPsec-compliant encryption (using DES, Triple DES, or other algorithms) and authentication (using MD5 or SHA-1) for either transport or tunnel mode. Either encryption, authentication, or both encryption and authentication can be used. Initially, manual keying is supported. Automated key management using ISAKMP and Oakley will be supported in future releases. In the initial release, the VPN feature is available in a U.S.-only version. An international version will be available in future releases.



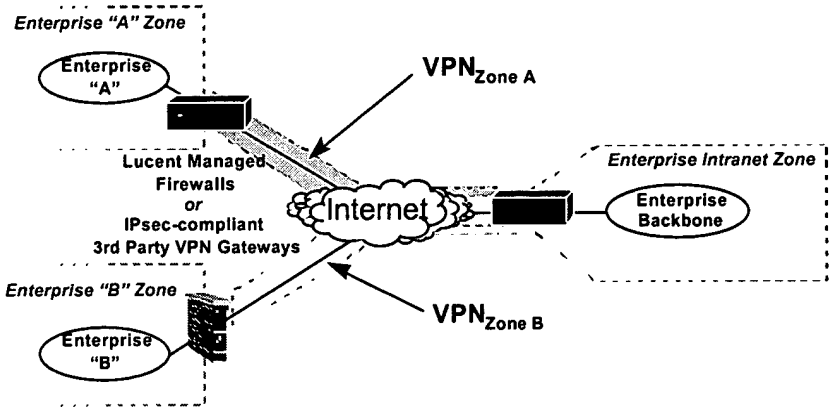
Multi-Customer Configuration

Internet Service Providers can use the Lucent Managed Firewall to offer enhanced firewall security as a value added service to their customers. In such a configuration, many firewall appliances can be centrally managed by the ISP using a single Security Management Server. Using the firewall's security zone feature, each customer can be assigned a separate security policy. The ISP can even allow customers to securely control their security policy without affecting any other security zones. For example, the ISP may want to allow the customer to create and edit their own policy and monitor their own audit records, but not to invoke or load changes to the policy without prior verification by the ISP. With the firewall's administrator privilege model, the ISP has the flexibility to easily implement this scenario.



Multi-Customer VPN Configuration

An enterprise or their service provider may need to set up VPNs at a moments notice with other enterprises (e.g., joint venture partners, suppliers, customers). The IPsec-compliant VPN feature in combination with the security zone feature supports this. For example, a separate security zone can be created by an enterprise for each external organization that the enterprise conducts electronic business with (e.g., Enterprise "A" and Enterprise "B"). In this manner, it is easy for the enterprise to define and manage a separate security policy governing communications with each distinct external business constituent. Furthermore, a distinct VPN can be created to protect communications with each external enterprise. Each VPN can be associated with the proper security policy. This approach is far easier to manage than the standard approach of adding special rules for each external enterprise to one super set of all possible rules.



Other Configurations

The scenarios presented above represent just a few typical enterprise and Internet Service Provider scenarios. Because the Lucent Managed Firewall provides such a rich and flexible feature set, we're certain that our customers will create innovative applications that we have not illustrated here and that cannot be easily done using any of the firewalls currently on the market. With the Lucent Managed Firewall, we think that the possibilities are endless.

For More Information

For more information on how to take advantage of the Lucent Managed Firewall's high level of security, scalability, and manageability, please visit the Lucent Managed Firewall web site at http://www.lucent.com/security.

For more information on the features available in version 2.0, please refer to the "Lucent Managed Firewall Version 2.0 Description of Product Features" document, posted to our web site.